

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA**

TIFFANIE BOWEN, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

HERITAGE VALLEY HEALTH SYSTEM,
INC.,

Defendant.

Case No. 2:23-CV-1320

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Tiffanie Bowen (“Plaintiff”) on behalf of herself and all others similarly situated, asserts the following against Defendant Heritage Valley Health System, Inc. (“HVHS” or “Defendant”), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

NATURE OF THE ACTION

1. This is a class action brought against HVHS on behalf of individuals impacted the HVHS’s unauthorized disclosure of their sensitive protected health information (“PHI”) to Meta Platforms, Inc. (“Meta”). Between approximately July 2018 and May 2023, HVHS procured and embedded an invisible 1x1 tracking pixel on its website and subpages, which then deployed on each website visitor’s internet browser for the purposes of intercepting and disclosing website visitor’s electronic communications with HVHS’s website to Meta.

2. The tracking pixel referred to as the Meta Pixel is a snippet of JavaScript code offered by Meta that can be embedded on a third-party website to track users’ actions as they navigate through the website. It logs the pages they visit, the buttons they click, the information

they type, and more.¹ The Meta Pixel then sends this harvested information to Meta, where it can be stored for years.²

3. When HVHS intentionally embedded the Meta Pixel on its website, and without its patients' knowledge or consent, HVHS shared with Meta every patient's interaction with its website. Meta then aggregated this data across all websites in order to build a dossier of that patient's activity, labeled with the patient's IP address, and matched to the patient's Facebook and/or Instagram account (or lack thereof).³

4. As a result of HVHS's use of the Meta Pixel, Plaintiff and Class Members' PHI, including information about their healthcare providers and services locations; types of conditions and treatments researched; computer IP addresses, and other personally identifying information was disclosed to Meta and other third parties without their authorization or consent.

5. As a healthcare provider, HVHS is required by law to provide every patient with a Notice of Privacy Practices. Defendant's HIPAA Privacy Notice states that "[i]t has been our practice not to disclose your medical information for any purpose without your written authorization" and further explains "[w]e are required by law to maintain the privacy of your protected health information."⁴

6. Despite HVHS's duty to safeguard and keep confidential its patients' PHI, HVHS nevertheless intentionally chose to procure and embed the Meta Pixel on its website, sharing

¹ Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

² *Facebook Business Tools Terms*, Facebook, <https://m.facebook.com/legal/terms/businessstools>, (last visited July 20, 2023).

³ *Id.*

⁴ *HIPAA Privacy Notice*, Heritage Valley Health System, <https://www.heritagevalley.org/patient-visitor-resources/hipaa-privacy-notice/> (last updated Dec. 2015).

Plaintiff's and Class Members' PHI with Meta without their consent when they interacted with Defendant's website.

7. The disclosure of such private information enabled Meta to gain deep insights into the types of medical care and treatment patients sought from HVHS.

8. As described throughout this Complaint, HVHS did not reasonably protect, secure, or store Plaintiff and Class Members' PHI, but rather intentionally and knowingly granted Meta access to confidential information that it knew or should have known was unlawful.

9. Accordingly, HVHS intentionally disclosed to Meta, and without authorization, Plaintiff's and Class Members' PHI, resulting in a significant invasion of patient privacy and a breach of confidentiality.

10. HVHS's actions constitute a reckless disregard for the privacy of its patients' PHI and its duties as a healthcare provider, an extreme invasion of Plaintiff's and Class Members' right to privacy, and violation of Pennsylvania statutory and common law.

11. Plaintiff, on behalf of herself, and the Classes as defined herein, brings claims for violations of the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S.A. §§ 5701, *et seq.*, breach of fiduciary duties, breach of confidence, and intrusion upon seclusion.

PARTIES

12. Plaintiff Bowen is an adult, who at all relevant times, is and was a citizen and resident of the Commonwealth of Pennsylvania.

13. Defendant HVHS is a Pennsylvania nonprofit corporation with a principal place of business located at 1000 Dutch Ridge Road, Beaver, Pennsylvania 15009.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

15. This Court has general personal jurisdiction over HVHS because its principal place of business is within the Commonwealth. Additionally, this Court has specific personal jurisdiction over HVHS because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in the Commonwealth.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because HVHS resides in this District and a substantial part of the events or omissions giving rise to the claim occurred within this District.

FACTUAL BACKGROUND

A. How the Meta Pixel Works.

17. In 2015, the Meta Pixel was announced as a tool to refine Meta's targeted advertising.

18. The Meta Pixel is a “sophisticated snippet of computer code” that is embedded in the overall code of a website or webpage.⁵ The Meta Pixel is a mechanism that loads JavaScript code which collects detailed and granular data for every interaction on a webpage.⁶

19. Once a third-party company, advertiser, or other entity sets up the Meta Pixel on a website, the Meta Pixel gathers valuable information about website visitors and the website activities.⁷ In turn, this allows advertisers to understand website users’ behaviors and shopping patterns, measure the performance of ad campaigns, and build an audience-base for future ad targeting.⁸

20. Meta also retains any information captured by the Meta Pixel and can use it for its own advertising purposes.⁹

21. Importantly, Meta designed the Meta Pixel such that Meta receives the information about a website user’s actions contemporaneously with those actions. This means that as soon as a website user takes any action on a webpage where the Meta Pixel is embedded, it discloses and redirects the user’s communications to Meta while the exchange of the communication between the website users and the website is still occurring.

⁵ Surya Mattu, Angie Waller, Simon Fondrie-Teitler, & Micha Gorelick, *How We Built a Meta Pixel Inspector*, The Markup (Apr. 28, 2022), <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>; *Get Started*, Meta for Developers, <https://developers.facebook.com/docs/meta-pixel/get-started/> (last visited July 12, 2023); *What Is A Tracking Pixel—Explained in 800 Words or Less*, DigitalMarketer (Sept. 17, 2019), <https://www.digitalmarketer.com/blog/what-is-tracking-pixel>.

⁶ Mattu et al, *supra* note 5.

⁷ Gloria Park, *What Are advertising Pixels – And Will They End With Third-Party Cookies?*, Viant (June 23, 2021), <https://www.viantinc.com/insights/blog/what-are-advertising-pixels-and-will-they-end-with-third-party-cookies/>.

⁸ DigitalMarketer, *supra* note 5.

⁹ Surya Mattu & Colin Lecher, *Applied for Student Aid Online? Facebook Saw You*, The Markup (Apr. 28, 2022), <https://themarkup.org/pixel-hunt/2022/04/28/applied-for-student-aid-online-facebook-saw-you>.

22. In response to congressional questioning in 2018, Meta stated that the Meta Pixel “provide[s] information about users’ activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook.”¹⁰

23. The Meta Pixel allows third parties to create a library which logs every time a website visitor takes an action (an “event”) that the third-party wants to track (a “conversion”). All of these tracked conversions are then stored so that the third-party can analyze the data collected.¹¹

24. The Meta Pixel collects standardized and customizable events. One such standard event will send packets of data that a person landed on a specific webpage.¹² Such information includes metadata information about a webpage, including the page title, URL, and page description.¹³ Metadata can be revealing because the titles or webpages or URLs visited can indicate what an individual searched for or viewed on a given webpage and such information can further serve as a proxy for personal data.

25. There are currently more than six million websites using Meta Pixel.¹⁴ On each of those websites, the Meta Pixel collects and sends information to Meta via scripts running in a person’s internet browser. That data is then delivered to Meta in “data packets” labeled with personally identifiable information (“PII”), including the user’s IP address.¹⁵

¹⁰ Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the Comm. on Com., Sci., and Transp., 94 Cong. 115 (2018) (Post-Hearing Questions).

¹¹ *Get Started*, Meta for Developers, <https://developers.facebook.com/docs/meta-pixel/get-started/> (last visited July 12, 2023).

¹² Mattu et al, *supra* note 5.

¹³ *Id.*

¹⁴ *Facebook Pixel Usage Statistics*, Built With, <https://trends.builtwith.com/analytics/Facebook-Pixel>, (last visited Nov. 4, 2022).

¹⁵ *Meta Pixel*, Meta for Developers, <https://developers.facebook.com/docs/meta-pixel/> (last visited July 12, 2023).

26. When a person visits a website where the Meta Pixel is embedded, the Meta Pixel will not only collect information about that person’s website activity, but will also match it to a person’s unique “c_user cookie.”¹⁶ When a person logs into their Facebook account “for the first time or from a new device, the c_user cookie is delivered to that [person’s] computer or device, and will be returned by the [person’s] web browser each time they interact with Meta.”¹⁷ Put differently, the “c_user cookie” enables the Meta Pixel to not only collect information, but to attribute the collected information to individual Facebook users, “effectively creating a ‘dossier’ that is recorded and utilized for future purposes.”¹⁸

27. If a person is not logged in to Facebook at the time, Meta uses personal information a user enters in form fields to match them to their Facebook and/or Instagram profile through a process called Advanced Matching.¹⁹ With this process, Meta collects emails, first and last names, phone numbers, birthdates, and addresses, then uses that information to connect event tracking data to a specific Facebook profile.²⁰

28. Even if a person does not have a Facebook account, has never registered for an account, has never so much as looked at a Facebook or Meta privacy policy, and has no intention to ever join any social media at all, Meta still collects data on that person. When asked by Congress about this maintenance of “shadow profiles” with data of nonusers of Facebook, Mark Zuckerberg

¹⁶ Offices of Sen. Elizabeth Warren, Ron Wyden, Richard Blumenthal, Tammy Duckworth, Bernie Sanders & Sheldon Whitehouse, & Representative Katie Porter, *Attacks on Tax Privacy: How the Tax Prep Industry Enable Meta to Harvest Millions of Taxpayers’ Sensitive Data* (July 2023), https://www.warren.senate.gov/imo/media/doc/Attacks%20on%20Tax%20Privacy_Final.pdf (“*Attacks on Privacy*”), at p. 7.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ Mattu et al, *supra* note 5.

²⁰ *Id.*

responded, “we collect data on people who have not signed up for Facebook for security purposes.”²¹

29. The Meta Pixel’s data collection abilities are quite concerning, especially if embedded on the websites of healthcare providers, as the Meta Pixel enables Meta to infer intimate details about an individual’s health conditions and deep insights into an individual’s activities simply by tracking an individual’s browsing activities on a healthcare provider’s website. Indeed, in June 2022, a Markup investigation revealed that hospitals across the country who embedded the Meta Pixel on their website were disclosing information about patients’ sensitive health information, including details about their medical conditions, prescriptions, and doctor’s appointments and sending that information to Meta.²² More concerning, however, is that since the Meta Pixel collects IP addresses and other PII, the information healthcare providers were disclosing to Meta could be linked to a specific individual or household.²³

30. While Meta purports to “hash” patients’ sensitive health information—obscuring them through a form of cryptography (or otherwise hiding the identifying information)—before sending the information to Meta, such claims of “anonymity” fail.

31. The Federal Trade Commission (“FTC”) has noted that “significant research has shown that ‘anonymized’ data can often be re-identified, especially in the context of location

²¹ Taylor Hatmaker, *Zuckerberg Denies Knowledge of Facebook Shadow Profiles*, TechCrunch (Apr. 11, 2018), <https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/>.

²² Feathers et al., *supra* note 1.

²³ *Id.*

data”²⁴ and former FTC Chief Technologist Edward Felten has found that “hashing is vastly overrated as an ‘anonymization’ technique.”²⁵

32. Similarly, security experts have also indicated that if user data is transmitted to Meta, “the hash method is not suitable for generating anonymous character strings.”²⁶ This is because “Meta explicitly uses the hashed information to link pixel data to Facebook profiles.”²⁷ During an interview with congressional staff, Meta admitted as much when it indicated that that it will match email addresses collected by the Meta Pixel to email addresses that Meta has on file.²⁸ Meta’s “c_user cookie” also enables Meta to connect the information collected by the Meta Pixel to specific Facebook profiles, thus allowing it to build dossiers on Facebook users.

B. HVHS Embedded the Meta Pixel on its Website.

33. HVHS “is a \$535 million integrated delivery network providing comprehensive health care for residents of Allegheny, Beaver, Butler and Lawrence counties, in Pennsylvania; eastern Ohio; and the panhandle of West Virginia.”²⁹

34. “In partnership with 3,800 employees and more than 600 physicians, [HVHS] offers a broad range of medical, surgical and diagnostic services at its three hospitals, Heritage

²⁴ Kristen Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, Fed. Trade Comm’n (July 11, 2022), <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>.

²⁵ Ed Felten, *Does Hashing Make Data “Anonymous”?*, Fed. Trade Comm’n (Apr. 22, 2012), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous>.

²⁶ *Attacks on Privacy*, *supra* note 16, at p. 14.

²⁷ Feathers et al., *supra* note 1.

²⁸ *Attacks on Privacy*, *supra* note 16, at p. 14.

²⁹ *About Heritage Valley*, Heritage Valley Health Network, <https://www.heritagevalley.org/about/overview/> (last visited July 12, 2023).

Valley Sewickley, Heritage Valley Beaver and Heritage Valley Kennedy; in 55 physician offices; and 21 community satellite facilities.”³⁰

35. HVHS operates the website and subpages of <https://www.heritagevalley.org/>.

36. HVHS’s website enables patients to “find a doctor,” “find a location”, and browse for various healthcare services Defendant offers at its numerous locations.

37. Between approximately July 2018 and May 2023, HVHS procured and embedded the Meta Pixel on its website. During this time, the Meta Pixel tracked patients’ website activities and simultaneously disclosed that information to Meta, who could then use the harvested information to infer intimate details about patients’ health.

38. Specifically, if a patient accessed Defendant’s website, the Meta Pixel secretly directed the patient’s internet browser to send a separate message to Meta’s servers. The second communication contained the original request that the patient sent to Defendant’s website, along with the additional data the Meta Pixel collected. This communication happened simultaneous with the first communication the patient initiated with Defendant’s website.

39. To illustrate this process, consider a patient who arrived at Defendant’s website and clicked on the “Services” tab. When the patient clicked this tab, their browser would send a request to HVHS’s server asking that the server load the “Services” subpage. Because HVHS embedded the Meta Pixel on its website, the Meta Pixel surreptitiously and contemporaneously duplicated the communication from the patient to HVHS and disclosed it to Meta along with information that can be used to identify the patient.

40. If the patient proceeded to click on a specific service, such as “Behavioral Health” that same process occurred again, enabling Meta to learn that the patient searched for behavioral

³⁰ *Id.*

health-related medical services. If the patient proceeded to click a specific location on the “Behavior Health” subpage, say “Staunton Clinic – Wexford,” Meta then learned the specific location the individual was looking for behavioral health services as the Meta Pixel collected the page title (Staunton Clinic – Wexford) and the page URL (<https://www.heritagevalley.org/locations/staunton-clinic-wexford-2/>).

41. Between July 2018 and May 2023, every time Defendant sent a patient’s data to Meta, the patient’s PHI was unlawfully disclosed. Indeed, HVHS could have chosen not to embed the Meta Pixel on its website, or it could have sought explicit authorization from patients before disclosing information to Meta, but Defendant did not.

42. Upon information and belief, as a result of HVHS’s decision to procure and embed the Meta Pixel on its website, it intercepted and disclosed to Meta the following: Plaintiff’s and Class Members medical providers and medical conditions and treatment; and PII that includes but is not limited to their location, IP addresses, and unique Facebook identifier.

43. HVHS therefore deprived Plaintiff and Class Members of their privacy rights by embedding and procuring the Meta Pixel to track and disclose Plaintiff’s and Class Members communications; by disclosing such information to Meta; and failing to obtain Plaintiff’s and Class Members’ consent to share their PHI with Meta.

C. Plaintiff and Class Members Have a Reasonable Expectation of Privacy Regarding Their PHI.

44. Plaintiff and Class members have a reasonable expectation of privacy in their data communicated to HVHS, including PHI.

45. As one law professor from the University of Michigan put it, the Meta Pixel’s surreptitious collection of sensitive health information “is an extreme example of how far the tentacles of Big Tech reach into what we think of as protected data space.”³¹

46. Another law professor characterized HVHS’s actions as “totally outside of the expectations of what patients think the health privacy laws are doing for them.”³²

47. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”³³

48. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.³⁴ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.³⁵

49. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual’s affirmative consent before a company collects and shares its customers’ data.

50. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing

³¹ Feathers et al., *supra* note 1.

³² *Id.*

³³ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

³⁴ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

³⁵ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.³⁶

51. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.³⁷

52. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.³⁸

53. Further HVHS is an entity covered under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1302d, *et seq.* (“HIPAA”), which sets minimum federal standards for privacy and security of protected health information.

54. Under 45 C.F.R. § 160.103, HIPAA defines “protected health information” or PHI as “individually identifiable health information” that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.”

55. Under 45 C.F.R. § 160.103, HIPAA defines “individually identifiable health information” as “a subset of health information, including demographic information collected from an individual” that is (1) “created or received by a health care provider;” (2) “[r]elates to the past,

³⁶ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

³⁷ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/>.

³⁸ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;” and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

56. HIPAA requires HVHS to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA’s security requirements. 45 C.F.R. §§ 164.102, *et seq.*

57. HIPAA further prohibits a healthcare provider from disclosing PHI with third parties, such as Meta, except where an individual has expressly consented in advance to the disclosure or under certain HIPAA-compliant contracts. According to a Health and Human Services’ Health Information Privacy Bulletin (“HHS Privacy Bulletin”), HIPAA-covered entities cannot share PHI to online tracking technology vendors for marketing purposes without entering into a HIPAA-compliant contracts or without first obtaining a patient’s HIPAA-compliant authorization.³⁹

58. The HHS Privacy Bulletin also indicates that patients may suffer a wide range of harms from a covered entity’s impermissible disclosure of a patient’s PHI, such as:

identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated

³⁹ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept’ of Health & Human Services (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#ftn19>.

entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.⁴⁰

59. According to HHS, HIPAA “[r]egulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity’s website or mobile app, including individually identifiable health information (IIHI) that the individual provides when they use regulated entities’ websites or mobile apps.” The information an individual provides may include “an individual’s medical record number, home or email address, or dates of appointments, as well as an individual’s IP address or geographic location, medical device IDs, or any unique identifying code.”⁴¹

60. All the above listed information that is collected on a regulated entity’s website, like HVHS’s website, is PHI, “even if the individual does not have an existing relationship with the regulated entity and even if the [individually identifiable health information], such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.”⁴² “This is because, when a regulated entity collects the individual’s IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual’s past, present, or future health or health care or payment for care.”⁴³

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

61. Given the application of HIPAA to HVHS and its website, Plaintiff and Members of the Class had a reasonable expectation of privacy in interactions with Defendant's website and their internet activities constitutes PHI provided to HVHS.

D. Plaintiff's and Class Members' Experiences.

62. Plaintiff has been a patient of HVHS since approximately 2011 and has a Facebook account.

63. While the Meta Pixel was embedded on HVHS's website, Plaintiff visited www.heritagevalley.org and certain of its subpages on her mobile phone numerous times while in Pennsylvania prior to the filing of this action.

64. While visiting HVHS's website, Plaintiff fell victim to Defendant's unlawful disclosure of her PHI to Meta using the Meta Pixel.

65. Unbeknownst to Plaintiff, HVHS procured and embedded the Meta Pixel on its website. In particular, the Metal Pixel was operative on HVHS's website and subpages during multiple visits by Plaintiff to Defendant's website.

66. During Plaintiff's visits to HVHS's website, Plaintiff browsed for doctors, healthcare facilities, and various services Defendant offers.

67. During these visits, the Meta Pixel instantaneously disclosed her PHI to Meta throughout her visit. Indeed, through HVHS's procurement of the Meta Pixel, Plaintiff's PHI was automatically and secretly disclosed while using Defendant's website, including an identifier unique to Plaintiff.

68. Thus, on multiple occasions when Plaintiff visited HVHS's website, her PHI was intercepted by the Meta Pixel and simultaneously disclosed to Meta who was then able to use the information to build a dossier on her.

69. The Meta Pixel operated in the same manner for all Class Members.

70. Like Plaintiff, each Class Member visited www.heritagevalley.org and/or its subpages with the Meta Pixel embedded in it, and the Meta Pixel intercepted and disclosed Class Members' PHI to Meta by sending packets of information to Meta.

71. The Meta Pixel procured by HVHS is an is an electronic, mechanical, or other analogous device for purposes of WESCA in that the Meta Pixel monitors, collects, and discloses the content of electronic computer-to-computer communications between Plaintiff's mobile computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website.

72. Alternatively, even if the Meta Pixel itself were not a device for purposes of WESCA, the Meta Pixel is software designed to alter the operation of a website visitor's computer or mobile phone by instructing the hardware components of that physical device to run the processes that ultimately intercept the visitor's communications and transmit them to Meta, without the visitor's knowledge.

73. The data collected by Meta Pixel reveals personalized and sensitive information about a patient's internet activity, habits, and medical care and treatment. As such, by the very nature of its operation, the Meta Pixel is a device used to intercept electronic communications.

74. The PHI intentionally collected and disclosed by the Meta Pixel was content generated through Plaintiff's and Class Members' use, interaction, and communication with HVHS's website relating to the substance and meaning of Plaintiff's and Class Members' communications with the website. This information is "content" as defined by WESCA and is not merely record information regarding the characteristics of the message that is generated in the course of the communication, nor is it simply information disclosed in the referrer headers. The

mere fact that Meta captures and values this information to gain insight on patient behavior confirms that the PHI is content that conveys substance and meaning to Meta.

E. Plaintiff and Class Members Did Not Consent to HVHS's Sharing of Their PHI With Meta.

75. Plaintiff and Class Members have no idea that HVHS was sharing their PHI when they interact with its website because the Meta Pixel is seamlessly incorporated into the background as the Meta Pixel is an invisible 1x1 tracking pixel.

76. For instance, when Plaintiff visited HVHS's website, there was no indication that the Meta Pixel was embedded on the website or that the Meta Pixel would collect or disclose her PHI. Specifically, HVHS does not ask patients to review its Privacy Policy upon arriving at its website nor does HVHS ask patients for permission to share their PHI with Meta when they arrive on the website.

77. Further, neither HVHS's HIPAA Privacy Notice nor its website's Privacy Policy furnish consent to share Plaintiff's and Class Members' PHI with Meta. HVHS's HIPAA Privacy Practice expressly states that "[i]t has been our practice not to disclose your medical information for any purpose without your written authorization"⁴⁴ It then contains vague references of when HVHS may share a patient's PHI, none of which permit HVHS to share PHI with Meta.⁴⁵

78. Similarly, HVHS's Privacy Policy expressly states "[w]e do not partner with or have special relationships with any Ad Network companies. This means we do not give your information to third parties for advertising or marketing purposes."⁴⁶ As such, HVHS expressly

⁴⁴ *HIPAA Privacy Notice*, *supra* note 4.

⁴⁵ *See id.*

⁴⁶ *Privacy Policy*, Heritage Valley Health System, <https://www.heritagevalley.org/privacy-policy/> (last updated Feb. 2006).

informs its patients that it does not share their PHI with advertisers, but nevertheless discloses their PHI with Meta in direct contradiction of such promises.

79. In any event, as an entity covered by HIPAA, HVHS does not have an unlimited right to share Plaintiff's and Class Members' sensitive health information with Meta.

80. Indeed, HVHS is not permitted to disclose PHI to a pixel tracking vendor based solely on its privacy policy, notice, or terms and conditions. Instead, HVHS is required to ensure that pixel tracking vendors, such as Meta, have entered into a Business Associate Agreement ("BAA") and there is an applicable permission prior to the disclosure of PHI. *See* 45 C.F.R. § 164.502(a) & 164.502(e).

81. Upon information and belief however, HVHS did not enter into a BAA with Meta that would permit sharing its patients' PHI with Meta.

82. Because there was no BAA with Meta in place while HVHS embedded the Meta Pixel on its website, HIPAA therefore required HVHS to obtain Plaintiff's and Class Members' express authorization to share their PHI with Meta **before** their PHI was disclosed to Meta. *See* 45 C.F.R. 508.⁴⁷

83. But as discussed above, neither HVHS's HIPAA Practice Notice nor its Privacy Policy provide any information to gain consent for HVHS to disclose Plaintiff's and Class Members' PHI to Meta. As such, HVHS disclosed Plaintiff's and Class Members' PHI to Meta without their consent.

F. HVHS Was Well Aware That It Was Disclosing Plaintiff's and Class Members' PHI to Meta.

84. HVHS was well aware that by procuring and embedding the Meta Pixel on its website, this would result in the disclosure of Plaintiff's and Class Members' PHI to Meta. By the

⁴⁷ HHS Privacy Bulletin, *supra* note 39.

very design of the Meta Pixel, *i.e.*, sending all interactions on a website to Meta, HVHS knew that its patients' PHI would be disclosed to Meta when they interacted with the website.

85. In June 2022, an investigation by the Markup revealed that the Meta Pixel iterations installed on hospital websites had been collecting patients' sensitive health information—"including details about their medical conditions, prescriptions, and doctor's appointments"—and sending it to Meta.⁴⁸ The Markup investigation further determined that the Meta Pixel shares with Meta, data from webpages with sensitive health information, including the URLs with the most obvious sexual health information—"post-abortion," "i-think-im-pregnant," and "abortion-pill."⁴⁹

86. One patient portal company, Epic Systems—the software company behind MyChart that provides access to medical records to hospitals—even "specifically recommended heightened caution around the use of custom analytics scripts."⁵⁰ Despite this, HVHS chose to embed the Meta Pixel on its website.

87. Further, the news is replete with the FTC bringing enforcement actions against companies for impermissibly sharing sensitive health information with Meta and other tracking pixel providers. For instance, the FTC reached a settlement with Flo Health, Inc., arising from allegations that the fertility-tracking app was sharing sensitive health information from millions of its users with marketing and analytics firms, including Meta and Google.⁵¹

⁴⁸ *Id.*

⁴⁹ Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, The Markup (June 15, 2022), <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>.

⁵⁰ Feathers et al., *supra* note 1.

⁵¹ *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, Fed. Trade. Comm'n (June 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

88. Likewise in February 2023, the FTC fined GoodRx, a telehealth and prescription drug provider, \$1.5 million for sharing customers' personal health information with tracking pixel vendors such as Meta, Google, and Criteo.⁵²

89. Similarly in March 2023, the FTC reached a \$7.8 million settlement with the online counseling service, BetterHelp, for sharing health data it promised to keep private, including information about mental health challenges, with Meta, Snapchat and other companies.⁵³

90. Moreover, HVHS was well aware that Meta's own data collection policies were insufficient to prevent the Meta Pixel from sharing HVHS's patients' sensitive health information with Meta. In February of 2021, New York State Department of Financial Services ("DFS") found that Meta collected sensitive health information in violation of its own policies. "Facebook acknowledged to DFS that, until DFS commenced its investigation, Facebook routinely obtained sensitive data from app developers, particularly in the area of health-related information, contrary to its own policies."⁵⁴ "The information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data."⁵⁵ "Merely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate fact is that Facebook does little

⁵² Annie Burky, *FTC slaps GoodRx with \$1.5M fine for sharing users' health data with Facebook, Google*, Fierce Healthcare (Feb. 1, 2023), <https://www.fiercehealthcare.com/regulatory/ftc-slaps-goodrx-fine-under-health-breach-notification-rule>.

⁵³ Frank Bajak, <https://apnews.com/article/betterhelp-ftc-health-data-privacy-befca40bb873661d1f8986bb75d8df07>.

⁵⁴ New York Department of Financial Services, *Report on Investigation of Facebook Inc. Data Privacy Concerns* (Feb. 18, 2021), https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_202.10218.pdf, at 7.

⁵⁵ *Id.* at pp. 7–8.

to track whether app developers are violating this rule and takes no real action against developers that do.”⁵⁶

91. Despite knowing that the Meta Pixel was sharing PHI with Meta when embedded on websites that provide health-related services—and knowing that Meta’s “policies” are woefully insufficient to screen medical information from being collected—HVHS still enabled the Meta Pixel on website and shared its patients’ PHI with Meta until at least May 2023, nearly 10 months after the Markup investigation revealed the Meta Pixel was sharing sensitive health information with Meta.

G. Plaintiff and Class Members Suffered Harm as a Result of the Illicit Disclosure of Their PHI.

92. The FTC has identified data collected about a person’s precise location and information about their health as the most sensitive categories of data collected. Standing alone, these data points “pose an incalculable risk to personal privacy” but when technology companies collect the data, combine it, and sell or monetize it, this amounts to an “unprecedented intrusion” and creates “a new frontier of potential harms to consumers.”⁵⁷

93. For example, the FTC recently reached a settlement with Flo Health, alleging the company shares sensitive health information about women collected from its period and fertility tracking app with Google and Meta, despite promising to keep this information private. FTC warns that the misuse use of such health information, including reproductive health data, exposes consumers to significant harm because: (1) criminals can use the health data to facilitate phishing scams or commit identity theft; (2) stalkers or other criminals can use the data to inflict physical

⁵⁶ *Id.* at p. 16.

⁵⁷ Cohen, *supra* note 324.

and emotional injury; and (3) the exposure of health information and medical conditions can subject people to discrimination, stigma, mental, anguish, and other serious harms.⁵⁸

94. As Chris Bowen, The Chief Privacy and Security Officer for ClearData, explained health information is so valuable because “[y]ou can build [an] entire human persona around a health record. You can create or seek medical treatment, abuse drugs, or get prescriptions.”⁵⁹ This is part of the reason why healthcare data may be valued at up to \$250 per record on the black market.⁶⁰

95. However, data is not just valuable to criminals. It is common knowledge that there is an economic market for consumers’ personal data, including the sensitive health information HVHS shared with Meta.

96. Healthcare providers, such as HVHS “sit on treasure troves: a stockpile of patient health data stored as electronic medical records.”⁶¹ These “files show what people are sick with, how they were treated, and what happened next.”⁶² Taken together, they’re hugely valuable resources for medical discovery.⁶³ When healthcare providers de-identify the records, *i.e.*, remove identifying information such as names, locations, and phone numbers, healthcare providers can sell the data to partners for research.

⁵⁸ *Id.*

⁵⁹ Will Maddox, *Why Medical Data is 50 Times More Valuable Than a Credit Card*, DMagazine (Oct. 15, 2019), <https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/>.

⁶⁰ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SecureLink (June 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers>.

⁶¹ Nicole Wetsman, *Hospitals are selling treasures troves of medical data – what could go wrong?*, The Verge (June 23, 2021), <https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research>.

⁶² *Id.*

⁶³ *Id.*

97. Unsurprisingly, healthcare groups have taken advantage of de-identifying medical records. The Mayo Clinic in Rochester, Minnesota is working with a startup to develop algorithms to diagnose and manage conditions based on health data.⁶⁴ Fourteen U.S. healthcare systems formed a company to aggregate and sell de-identified data.⁶⁵ And one hospital chain even researched an agreement with Google to use patient data to develop healthcare algorithms.⁶⁶

98. Given the monetary values of sensitive health information, HVHS deprived Plaintiff and the Class Members of the economic value of their PHI by sharing such data without providing proper consideration for Plaintiff's and Class Members' property.

CLASS ACTION ALLEGATIONS

99. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

Nationwide Class: All natural persons in the United States whose personal information was collected through the use of the Meta Pixel embedded on www.heritagevalley.org.

Pennsylvania Subclass: All natural persons in the Commonwealth of Pennsylvania whose personal information was collected in Pennsylvania through the use of the Meta Pixel embedded on www.heritagevalley.org.

100. Excluded from the Classes are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Classes, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ Nicole Westman, *Google to use patient data to develop healthcare algorithms for hospital chain*, The Verge (May 26, 2021), <https://www.theverge.com/2021/5/26/22454817/google-hca-patient-data-healthcare-algorithms>.

101. These proposed class definitions are based on the information available to Plaintiff at this time. Plaintiff may modify the class definitions in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

102. **Numerosity:** The members of the Classes are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of HVHS or Meta.

103. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to:

- a. Whether Meta Pixel is designed to send individually identifiable information from HVHS to Meta;
- b. Whether HVHS violated Plaintiff's and Class Members' privacy rights;
- c. Whether HVHS's transmittal to Meta of the contents of electronic communications between patients and HVHS occurred contemporaneous to their making;
- d. Whether HVHS intercepted and/or transmitted to Meta the contents of electronic communications between patients and HVHS without Plaintiff's and Class Members' consent;
- e. Whether HVHS's actions violated WESCA, 18 Pa. C.S.A. §§ 5701, *et seq.*; and
- f. Whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

104. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Classes. The claims of Plaintiff and the members of the Classes arise from the same conduct by Defendant and are based on the same legal theories.

105. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Classes. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Classes, and Defendant has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Classes.

106. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

107. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example,

Defendant's liability and the fact of damages is common to Plaintiff and each member of the Classes.

108. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's and/or Meta's books and records.

CAUSES OF ACTION

COUNT I

Violation of WESCA

18 Pa. C.S.A. §§ 5701, *et seq.*

(On behalf of Plaintiff and the Classes)

109. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

110. Plaintiff brings this claim individually and on behalf of the Classes.

111. WESCA prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. C.S.A. § 5703.

112. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of WESCA is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. C.S.A. § 5725(a).

113. “Intercept” is defined as any “[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 18 Pa. C.S.A. § 5702.

114. “Contents” is defined as “used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication.” 18 Pa. C.S.A. § 5702.

115. “Person” is defined as “any individual, partnership, association, joint stock company, trust or corporation.” 18 Pa. C.S.A. § 5702.

116. “Electronic Communication” is defined as “[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.” 18 Pa. C.S.A. § 5702.

117. HVHS is a person for purposes of WESCA because it is a corporation.

118. The Meta Pixel procured by HVHS is a “device” used for the “acquisition of the contents of any wire, electronic, or oral communication” within the meaning of WESCA. Courts have held that software constitutes a “device” for purposes of applying wiretap statutes. *See, e.g., United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a device); *Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a “device” for the purpose of the Wiretap Act); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an “electronic, mechanical or other device”); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661-62 (E.D. Ten. 2012) (analyzing spyware software as a device under Wiretap Act); *Shefts v. Petrakis*, 2012 WL 4049484, at *8-9 (C.D. Ill. 2012) (analyzing software as a device under the Wiretap Act).

119. Alternatively, even if the Meta Pixel itself were not consider a “device” under WESCA, the Meta Pixel ultimately “uses” the physical computers and mobile phones of Plaintiff and Class members and by instructing those devices to run the physical processes necessary to accomplish the interception and disclosure of Plaintiff’s and Class Members’ communications and transmission of those communications to Meta.

120. HVHS intentionally procured and embedded the Meta Pixel on its website to spy on, automatically and secretly intercept and disclose Plaintiff’s and Class Members’ electronic communications with HVHS in real time to Meta.

121. Plaintiff’s and Class Members’ PHI communicated with HVHS’s website are exchanges of electronic communications under WESCA as they include the URL of the webpages visited, titles of webpages visited, doctors searched for, and medical treatments and conditions viewed. *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) (“If an address, phone number, or URL is . . . part of the substantive information conveyed to the recipient, then by definition it is ‘content.’”); *see also In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 936, 949 (N.D. Cal. June 13, 2022) (finding that categories of the website, categories that describe the current section of the website, and referrer URL that caused navigation to the current page constituted “content”).

122. Plaintiff’s and Class Members’ intercepted PHI therefore constitute the “contents” of electronic communication[s]” within the meaning of WESCA.

123. Plaintiff’s and Class Members’ electronic communications are intercepted contemporaneously with their transmission.

124. Plaintiff and Class Members did not consent to having their PHI intercepted and disclosed by the Meta Pixel.

125. Pursuant to 18 Pa. C.S.A. 5725(a), Plaintiff and the Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

COUNT II
Invasion of Privacy – Intrusion Upon Seclusion
(On behalf of Plaintiff and the Classes)

126. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

127. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

128. Plaintiff brings this claim individually and on behalf of the Classes.

129. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

130. Plaintiff and Class Members did not consent to, authorize, or know about HVHS's intrusion at the time it occurred. Plaintiff and Class Members never agreed that HVHS could disclose their PHI to Meta.

131. Plaintiff and Class Members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

132. HVHS's intentionally intruded on Plaintiff's and Class Members' private life, seclusion, or solitude, without consent by disclosing their PHI to Meta.

133. HVHS conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

134. Plaintiff and Class Members were harmed by HVHS's wrongful conduct as HVHS's conduct has caused Plaintiff and Class Members mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

135. HVHS's conduct has needlessly harmed Plaintiff and the Classes by capturing intimately personal facts and data in the form of their PHI. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

136. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class Members of the economic value of their PHI, without providing proper consideration for Plaintiff's and Class Members' property.

137. As a direct and proximate result of HVHS's conduct, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Classes)

138. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

139. Plaintiff brings this claim individually and on behalf of the Classes.

140. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI that was conveyed to and collected by HVHS, and ultimately disclosed to Meta without Plaintiff's or the Class Members' consent.

141. As a healthcare provider, HVHS has a fiduciary relationship to its patients, like Plaintiff and the Class Members.

142. Because of that fiduciary and special relationship, HVHS was provided with Plaintiff's and Class Members' PHI, and owes them, at a minimum, a duty of confidence and confidentiality.

143. HVHS owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, safeguarding, and protecting their PHI in its possession from being disclosed to unauthorized persons, such as Meta.

144. HVHS breached the duties owed to Plaintiff and Class Members by procuring and embedded the Meta Pixel on its website and disclosing Plaintiff's and Class Members' PHI without their consent to Meta.

145. But for HVHS's wrongful breach of its duties owed to Plaintiff and Class Members, their PHI would not have been disclosed.

146. As a direct result of HVHS's breach of its fiduciary duty, Plaintiff and Class Members have suffered injuries, including but not limited to:

- a. Damages that will reasonably compensate Plaintiff and Class members from the harm to their privacy interests in their PHI;
- b. Damages that will reasonably compensate Plaintiff and Class members for the breach of their confidences and the erosion of their confidential relationship between patient and healthcare provider; and
- c. Emotional distress from the unauthorized disclosure of their PHI to Meta.

147. As a direct and proximate result of HVHS's breach of its fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
Breach of Confidence
(On behalf of Plaintiff and the Classes)

148. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

149. Plaintiff brings this claim individually and on behalf of the Classes.

150. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI that was conveyed to and collected by HVHS, and ultimately disclosed to Meta without Plaintiff's or the Class Members' consent.

151. As a healthcare provider, HVHS has a special relationship with its patients, like Plaintiff and the Class Members.

152. Because of that special relationship, HVHS was provided with private and valuable PHI related to Plaintiff and the Class, which it was required to maintain in confidence.

153. Plaintiff and the Classes provided HVHS with their personal and confidential PHI under both the express and/or implied agreement of HVHS to limit the use and disclosure of such PHI.

154. HVHS owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

155. HVHS had an obligation to maintain the confidentiality of Plaintiff's and Class Members' PHI. That obligation is demonstrated by above described sources, such as HVHS's HIPAA Privacy Notice and HIPAA.

156. Plaintiff and Class Members have a privacy interest in their personal medical matters, and HVHS had a duty not to disclose confidential medical information and records concerning its patients.

157. As a result of the parties' relationship, HVHS had possession and knowledge of confidential PHI of Plaintiff and Class Members.

158. Plaintiff's and Class Members' PHI is not generally known to the public and is confidential by nature.

159. Plaintiff and Class Members did not consent to nor authorize HVHS to release or disclose their PHI to Meta

160. HVHS breached the duties it owed to Plaintiff and Class Members by procuring and embedding the Meta Pixel on its website, which intercepted and disclosed Plaintiff's and Class Members' PHI to Meta without their consent or authorization.

161. But for HVHS's wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PHI would not have been disclosed to Meta.

162. As a direct and proximate result of HVHS's breach of Plaintiff's and Class Members' confidences, Plaintiff and Class Members have suffered injuries, including:

- a. The erosion of the essential and confidential relationship between HVHS—as a healthcare provider—and Plaintiff and Class Members as patients;
- b. Loss of their privacy and confidentiality in their PHI; and
- c. Emotional distress from the unauthorized disclosure of their PHI to Meta.

163. As a direct and proximate result of HVHS breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages in an amount to be proven at trial.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Classes, respectfully request that the Court enter judgment in Plaintiff's and the Classes favor and against Defendant as follows:

- A. Certifying the Classes and appointing Plaintiff as the Class representative;
- B. Appointing Plaintiff's counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Awarding Plaintiff and the Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- E. Awarding Plaintiff and the Class Members pre-judgment and post-judgment interest;
- F. Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and
- G. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Classes, demands a trial by jury of any and all issues in this action so triable of right.

Dated: July 21, 2023

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch

Nicholas A. Colella

Patrick D. Donathen

LYNCH CARPENTER, LLP

1133 Penn Ave., 5th Floor

Pittsburgh, PA 15222

Telephone: (412) 322-9243

gary@lcllp.com

nickc@lcllp.com

patrick@lcllp.com

Attorneys for Plaintiff